

足りぬ人材 連携も未知数



下

ハイブリッド戦募る危機感

「史上初めてアクティ
ブ・サイバー・ディフェ
ンス(ACD)を発動す
る」。「首相」の小野寺
五典・元防衛相は唐並ぶ
「閣僚」らに訴えた。
「大変重要な決定だが、そ
れだけ烈度の高いサイバ
ー攻撃を受け、国民生活
が大混乱している」

2023年7月、国会
議員が閣僚役などを務め
て自衛隊元幹部も現役幹
部役として参加し、台湾
有事が実際に起きた想定
で日本政府がどう行動
するべきかをシミュレ
ーションしたイベント(民
間シンクタンク「日本戦
略研究フォーラム」主
催)が行われた。想定で
は、沖縄電力や九州電力
がサイバー攻撃でランサ
ムウェア(身代金ウイル
ス)に感染し、停電が

発生。「官房長官」役の
長島昭久・現首相補佐官
は「中国の関与が特定
された場合、自衛隊は
ITインフラの無力化を
実施し、サイバー攻撃を
遮断して欲しい」と「防
衛相」に要請。小野寺
「首相」は「サイバー
攻撃は『ハイブリッド
戦』の一環だ」と強調し
た。

ハイブリッド戦とは、
サイバーや情報戦など多
様な手段を組み合わせて
敵を攻撃することを指
す。現実の日本を取り巻
く安保環境についても、
ある政府関係者は「サイ
バー空間では、もはや有
事に近い状況がはじまっ
ている」と指摘する。能
動的サイバー防御(ACD)
の導入は、台湾有事
におけるハイブリッド戦
も念頭に置いた動きだ。
政府が危機感を抱いた
きっかけの一つは、22年

日本のサイバー防御体制の課題

	サイバー専門部隊 2027年度までに自衛隊のサイバー専門部隊を約4千人に増員する計画 ↓ 約3万人とされる中国に数で劣る	
	待遇 民間の待遇に劣り、専門人材の獲得に苦戦	
	指揮系統 指揮系統が異なる警察と自衛隊の連携がどこまで進むか未知数	

2月のロシアによるウクライナ侵襲だ。
ウクライナでは14年のロシアによるクリミア併合以降、大規模なサイバー攻撃で停電などの被害が毎年発生。これを受け、通信インフラの分散化などの自助努力のほか、米国の支援も受け、サイバー防御能力の向上に力を入れてきた。

英紙フィナンシャル・タイムズによると、21年10月には米軍のサイバー部隊がウクライナを訪れ、鉄道システム内に埋め込まれた不正なプログラムを除去した。ロシアによる侵襲直前には、政府機関の重要データをネットのクラウド上に移す法整備に踏み切り、首都キーウ中心部に

にあった政府のデータセンターが侵襲直後にミサイルで破壊されても政府機能を継続できたという。

防衛省出身でウクライナ情勢に詳しい松原実穂子NTTチーフ・サイバーセキュリティ・ストラテジストは、鉄道は国民の避難や支援助物資の輸送に大きく役立ったとし、「軍事侵襲に合わせて鉄道機能が止められていたら、ウクライナの継続能力に相当な打撃が出たのではないかと指摘」。「ウクライナは(クリミア併合の)14年から8年間かけ、サイバー防御能力を高めた。日本もあらゆるシナリオを想定し、平時から官民が連携してサイバー防御能力を高めるべきだ」と話す。

日本のサイバー防御能力をめぐっては課題が山積している。一つは、人材不足だ。自衛隊は専門部隊を22年度の890人から27年度までに約4千人に増やす計画だが、約3万人ともされる中国の部隊と比べると圧倒的に少ない。人材獲得に苦戦

「給与など待遇面が良い民間には太刀打ちできない」と漏らす。

二つ目が、自衛隊と警察との連携だ。ともにサイバー防御を担う両組織の間では、相互のサイバー訓練の視察が始まっている。ただ、(1)1936年の(2)26事件以来、警察と自衛隊は因縁が深い(政府関係者)との見方もあるように、両組織は複雑な関係を持ち、指揮系統の異なる両組織の連携がどこまで進むか未知数だ。

自衛隊制服組トップの吉田圭秀・統合幕僚長は2月の記者会見で、日本のサイバー防御能力の現状についてこう率直に語った。「攻撃側の能力が日々向上し、我々が今のままで対応できるとは認識していない」

様々な課題を抱えるACD法案は、来週中にも衆院で審議入りする。政府による情報収集のあり方やプライバシー保護などをめぐり、国会でどのような論議が交わされるのか。重要な局面を迎えている。

(田嶋慶彦、矢島大輔、鈴木 峻)